PARTNERSHIP WITH THE CINCS IN THE YEAR 2000 (Y2K) OPERATIONAL EVALUATIONS

I. WHAT WE ACCOMPLISHED

Anticipating the approach of the Year 2000 and the potential for catastrophic computer system problems, the Department of Defense began an extensive project intended to forestall trouble. Investing some $3.6 billion over five fiscal years, the Services, Agencies, and the Unified Commands looked into all possible areas where the millennium bug might appear. This effort culminated in an extensive series of operational evaluations (OPEVAL) by the Unified Commands that found few substantive Y2K problems, but did disclose some important interoperability problems. Although DoD had expected to unearth a lot of Y2K difficulties, the real benefit of the effort was to point out the need for continued attention to interoperability in our complicated command, control, communications, computer, and intelligence (C^4I) system of systems.

Spending such a large amount of money brought with it the question, "Was it worth it?" It was, but not only for the Y2K problems that were solved. The greatest benefit came first in having the various CINCs determine the *thin lines* of mission critical command and control system architectures and then in verifying warfighting system interoperability via the operational evaluations. Thin lines are those minimum essential C^4I systems that allow each command to meet its critical mission and operational requirements; they are the linchpin of operations in a Y2K environment. Without this C^4I system of systems, modern military operations would not be possible. Moreover, the concept of defining and understanding the C^4I thin lines did not exist before DoD undertook this Y2K evaluation effort; how ready the commands would have been for war in the Year 2000 without the corrections we made is problematical. However, we have made substantial improvements in understanding our C^4I system interoperability which might never have been motivated or funded had it not been for the DoD Y2K effort.

In 1998, acting on instructions from the Secretary of Defense, the Chairman of the Joint Chiefs of Staff directed the CINCs to undertake Y2K OPEVALs to demonstrate their ability to conduct military operations during the Y2K transition period. The Deputy Secretary of Defense asked DOT&E to provide assistance to warfighting CINCs in planning and conducting these OPEVALs. DOT&E began work on this project in June 1998.

Nine CINCs participated in the Y2K OPEVAL process. Included were the Joint Forces Command (JFCOM) formerly called Atlantic Command (ACOM), Central Command (CENTCOM), European Command (EUCOM), Pacific Command (PACOM) with U.S. Forces Korea (USFK) as a major warfighting component of PACOM, Special Operations Command (SOCOM), Southern Command (SOUTHCOM), Space Command (SPACECOM)/North American Aerospace Defense Command (NORAD), Strategic Command (STRATCOM), and Transportation Command (TRANSCOM).

Through extensive OPEVAL planning, DoD identified 2,107 mission critical systems and 4,749 non-mission critical systems. Of the 2,107, the Joint Staff included 452 in their Master CINC Thin Line List as primary systems to be addressed during the CINC Y2K OPEVALs. Of the 452 systems, 94 did not have a date processing function or were deemed to be *trusted*. Per paragraph 1.2, page 1-3, Appendix I---Guidelines to Support DoD Y2K Operational Readiness, to the DoD Y2K Management Plan, v2.0, dated March 1999, the definition for a Trusted System is: "Some mission-critical systems that process dates can not be taken off-line without potentially causing adverse impacts to real-world operations.

Additionally, these systems can not be otherwise simulated in a reasonable Y2K operational testing environment." Unfortunately, at least one trusted system did fail during the midnight crossing. Table 1 depicts those excluded from evaluations. The individual Services or Agencies tested and evaluated the remainder of the 2,107, and were responsible for ensuring they were Y2K compliant.

Table 1. System Exclusions from CINC OPEVAL Testing

Exclusion Category	Number of Systems
Trusted Systems	**16**
No Date Processing Systems	**78**
Total Exclusions	**94**

Some of the most commonly recurring systems in the evaluations were the local area networks (LANs), various electronic mail applications, secure and normal voice telephone and facsimile, the secret Internet protocol (SIPRNET), and the unclassified but sensitive Internet protocol (NIPRNET). In addition, each command had a number of unique programs and applications that they evaluated. The most commonly encountered systems and applications were as follows:

- **Global Command Control and Related Systems or Applications**
  - AMHS — Automatic message handling systems (of several types including projected replacements for currently used systems.
  - GCCS — Global Command and Control System, including its Army, Maritime and Korea versions, the Common Operational Picture (COP), and the Joint Operational Planning and Execution System (JOPES)
  - GTN — Global Transportation Network
  - JTAV — Joint Total Asset Visibility
  - CTAPS — Contingency Tactical Air Control System Automated Planning System
  - AFATDS — Army Field Artillery Tactical Data System
  - Microsoft Office®, Internet Explorer®, and Windows/Windows NT®
  - Netscape Navigator®

- **Intelligence Related Systems and Applications**
  - Anchory: an interactive storage and retrieval system
  - ASAS — All Source Analysis System
  - Coliseum – Community On-Line Systems for End Users and Managers
  - INTELINK and INTELINK/S
  - IPA/IPL — Imagery Product Archive/Imagery Product Library
  - JDISS — Joint Defense Intelligence Support System
  - MIDB — Modernized Integrated Data Base
  - Oilstock: software for digital map data manipulation
  - 5D — Demand Driven Direct Digital Dissemination

- **Communications**
  - AUTODIN — Automatic Digital Network
  - DSN/DRSN — Defense Switched Network/Defense Red Switched Network
  - JWICS — Joint Worldwide Intelligence Communications System
  - Commercial telephone and facsimile systems

In general, the OPEVALs were very successful. The commands evaluated the performance of LANs, planning and mission support systems or applications such as the Joint Tactical Information Distribution System, mission-planning systems like the Contingency Tactical Air Control System and its projected replacement, as well as automatic message handling systems. The commands also evaluated intelligence support systems, for example, INTELINK and the Imagery Product Archive/Imagery Product Library. OPEVALs detected a total of 34 hard failures (obvious adverse impact to the system and/or process) and eight soft failures (system and/or process impact is not immediately discernable). The commands referred the Y2K problems observed to the appropriate developers or system managers for resolution.

Most OPEVALs did not last long enough to check for soft failures over a period of days. Once an OPEVAL was completed, the network was torn down and the hardware and software scrubbed for return to normal operation. Subsequently, additional soft failures were identified through detailed analysis of data collected in preparation for the 30-day report to the Joint Staff. The focus during OPEVALs was on the hard failures, and then on the soft failures that could be identified during execution of OPEVAL, followed by other problems that surfaced. Y2K related hard failures received immediate attention for fixing. Non-Y2K related problems were also addressed as resources and the nature of the failure permitted. The commands completed some fixes immediately and some required problem reports sent to the respective program manger for resolution. Table 2 depicts the type of Y2K faults noted and the actions taken to fix them.

Table 2. CINC OPEVAL System Failures

			STATUS				
CINC	**Hard Failure**	**Soft Failure**	**Fixed H / S**	**Under Review H / S**	**Delayed Fielding H / S**	**Fix Planned H / S**	**No Action H / S**
JFCOM	3	0	3/0	0	0	0	0
CENTCOM	5	0	1/0	1	2	0	1
EUCOM	2	0	2 / 0	0	0	0	0
PACOM	2	0	2 / 0	0	0	0	0
USFK	5	0	2 / 0	0	0	1	2
SOCOM	3	0	0 / 0	0	0	1	2
SOUTHCOM	1	0	1 / 0	0	0	0	0
SPACECOM	4	4	2 / 3	2 / 0	0 / 0	0 / 0	0 / 1
NORAD	1	2	1 / 2	0	0	0	0
STRATCOM	0	0	0	0	0	0	0
TRANSCOM	8	2	5 / 0	0 / 1	0 / 0	0 / 1	3 / 0
TOTAL	**34**	**8**	**19 / 5**	**3 / 1**	**2 / 0**	**2 / 1**	**8 / 1**

Legend:

H / S = Hard Failure/ Soft Failure

No Action = No Action Taken; No good fix currently available; No fix planned; or No fix–System to be Replaced.

Throughout the OPEVALs, two issues regularly appeared among the commands. First was the need for continuous configuration management. Configuration management was vital in ensuring that the command had installed and used only Y2K-certified systems/applications. Often, agencies or offices installed new or different applications/programs on their computers. These differences prevented locations/offices from communicating with each other until applications were standardized. Despite efforts to control configuration management, another difficulty cropped up regularly. That issue was incompletely addressed or unresolved problems with joint interoperability. Joint interoperability problems arose because many commands and Services employed systems that, although aimed at similar goals, were not interoperable or could not be accessed or used by other systems. This caused needless duplication and work. These problems overlapped when commands or components used different versions of the same application or system, making them partially or entirely incompatible.

The commands also encountered an old problem: organizations had failed to regularly exercise their system capabilities to ensure that they worked. For example, one of the commands held a rehearsal of staff activities for the Y2K rollover period. This command intended to use satellite communication terminals and Ultra High Frequency/Extremely High Frequency radios in the event computer-based systems failed. These stored backup systems had not been used for an extended time period, several years for some equipment. When the rehearsal began, personnel discovered that the equipment had not been used for so long that *none* of the alternate communications worked. Several days elapsed before parts could be obtained to correct the equipment problems or bring the equipment up to date.

Since the command, control, communications, computers, intelligence, surveillance, and reconnaissance (C^4ISR) infrastructure is in a state of continual improvement and the OPEVALs were instrumental in identifying C^4ISR architectures and thin line critical systems, the Department should consider institutionalizing periodic OPEVALs every three or four years. Several agencies should assist in these evaluations, including the new Director of Interoperability, the Joint Interoperability Test Center (JITC), Joint Forces Command, and DOT&E. These periodic exercises would provide opportunities for the Unified Commands' to update assessments of their ability to meet mission requirements, verify interoperability of existing systems and new programs, and identify those systems that could be eliminated. Consistently, all of the commands found that personnel and agencies believed they were working with similar or identical programs, but in fact were not. Accordingly, their systems could not always interoperate. These OPEVALs illustrated the importance of regularly exercising the systems to ensure emergency readiness.

All commands increased their knowledge of their current capabilities and how they can improve them. Perhaps the most important benefit learned was the work required to prepare for the exercises. To prepare for OPEVALs, the commands identified their critical missions, subordinate critical mission support tasks, and then developed thin lines according to their mission requirements. Thus, a major result of Y2K OPEVALs were the definition and critical review by the Unified Commands of their C^4ISR infrastructure from an operational capability *vice* technical capability perspective. Upon analyzing their enterprise processes, the CINCs found only a third of their systems (on average) to be critical.

At the conclusion of the OPEVALs, some residual risks in terms of telephone, power, and host nation support remained. An unknown potential for system of system interaction problems remained because of the inherent complexity of the network of computer-based systems. The commands could not address all of these issues, so they trained standby teams to be available at the date rollovers to implement necessary corrections or operational contingency plans. Overseas areas such as Italy, Greece, and Spain posed potential problems in areas such as electrical power supply and air traffic control. The commands worked with host country officials to assess their risks and identify potential problems.

II. DOT&E SUPPORT FOR CINC OPEVALS

DOT&E provided support for Y2K verification activities worldwide, including expert assistance for cross-functional, inter-Service, and cross-system testing. The amount of effort that DOT&E provided varied by command, and was governed by the nature and complexity of each situation. For example, EUCOM was heavily involved with the air war over Serbia, and DOT&E representatives assisted in key OPEVAL planning and conduct of the operational evaluations. Due to the rapid turnover of personnel assigned to Korea and the relatively small staff there, DOT&E, along with contractor support, provided substantial support to the evaluation planning and assessment team. DOT&E significantly contributed to the OPEVAL planning and execution to all commands.

In September 1998, DOT&E and the Service Operational Test Agencies (OTA), particularly the Air Force Operational Test and Evaluation Center, began the Y2K project using their own funds. To meet this unfunded requirement, DOT&E requested $61 million to provide additional resources for DOT&E and OTAs. In March 1999, $12.9 million was made available and distributed among all four Service OTAs and JITC to support the CINCs. Approximately 60 people assisted the commands. The OTA/command support focus areas were as follows:

- OPTEVFOR JFCOM, PACOM, TRANSCOM
- AFOTEC STRATCOM, SPACECOM/NORAD, EUCOM
- OPTEC/MCOTEA CENTCOM, SOUTHCOM, SOCOM, USFK
- JITC All Commands
- DOT&E All Commands

Figure 1 shows how the Services and CINCs focused their Y2K activities. The Service tests of individual systems were at the program manager and command function levels. These tests were the basis for certifying individual systems as Y2K compliant. Subsequent CINC OPEVALs concentrated on mission-level activities, and primarily tested compliant systems for system to system interoperability in executing critical missions. Each CINC, however, supervised testing of the thin lines from sensor to shooter by its components and supporting agencies.

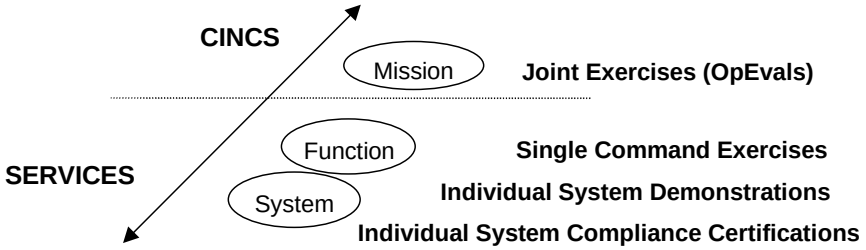

Figure 1. Service and CINC Y2K Verification Activities

The participation of DOT&E and the OTAs in the OPEVALs drew upon their experiences in planning and conducting operational testing and evaluation. We helped the CINCs refine their methods and provided support for executing OPEVALs. Depending on the particular CINC, DOT&E assisted in test planning, training, rehearsal, execution, analysis, and/or reporting. Table 3 summarizes by command the critical mission areas examined during CINC OPEVALs. The table also includes the number of OPEVALs in each of the Commands, however, bear in mind that some Commands, such as TRANSCOM, supported other CINC OPEVALs. Although TRANSCOM shows four OPEVALs, one was in conjunction with CENTCOM.

III. OPEVAL METHODOLOGY

Using Joint Staff guidance, each command developed its own fundamental evaluation methodology. This consisted of sending messages, data, and images (referred to as products) through the thin lines of systems on the following critical midnight crossings: December 31, 1999-January 1, 2000, February 28-29, 2000, and February 29-March 1, 2000. Evaluators gauged the effects of the clock rolls relative to baseline data collected prior to entering the simulated Y2K environment.

The end-to-end evaluation of each thin line required detailed planning to accurately reflect the critical tasks, functions and methods by which the commands accomplished their critical missions. The CINCs employed product inputs and associated outputs using realistic tasks and message traffic to evaluate the systems in the simulated Y2K environment.

Table 3. Summary of Missions Assessed during CINC OPEVALs

CINC	CRITICAL MISSIONS	Number of OPEVALs
JFCOM (ACOM)	Force Provider Area of Responsibility (AOR)	5
CENTCOM	Major Theater War (MTW); Intelligence Surveillance and Reconnaissance (ISR); Reception, Staging Onward Movement, and Integration; Theater Missile Defense (TMD);	2
EUCOM	Peacekeeping Operations (PKO); Non-combatant Evacuation Operations (NEO)	3
PACOM	En route C2, Initial Entry; MTW	3
USFK	MTW	2
SOCOM	Alert, Deployment, Planning/Execution	5
SOUTHCOM	Counter Drug	3
SPACECOM/ NORAD	Tactical Warning/Attack Assessment (TW/AA); Space Support/Operations	15/2
STRATCOM	Nuclear C^2	5
TRANSCOM	Deployment Sustainment	3

An accurate system configuration was essential to determine where to collect the products along each thin line. In some cases, due to operational considerations, the CINCs used parallel systems isolated from the operational networks by network encryption systems (NES). This minimized any potential corruption or distortion of systems handling critical, real-world command and control information.

To ensure the system configuration, the CINCs developed architectural diagrams depicting the systems in each thin line along with associated functional flow diagrams. These diagrams were helpful in depicting the transfer of the products through the sites and information systems, including the backbone networks.

The USFK team, for example, found that the depictions of the architectures did not accurately illustrate the data capture points along each thin line, nor did they show how data would be captured (i.e.,

soft copy, hard copy, or direct observation). To provide this level of detail, the USFK team developed an independent bit path for each of their thin lines. The bit paths identified the exact flow of products from originator, through every component, to the end user. A sample bit path is illustrated in Figure 2.

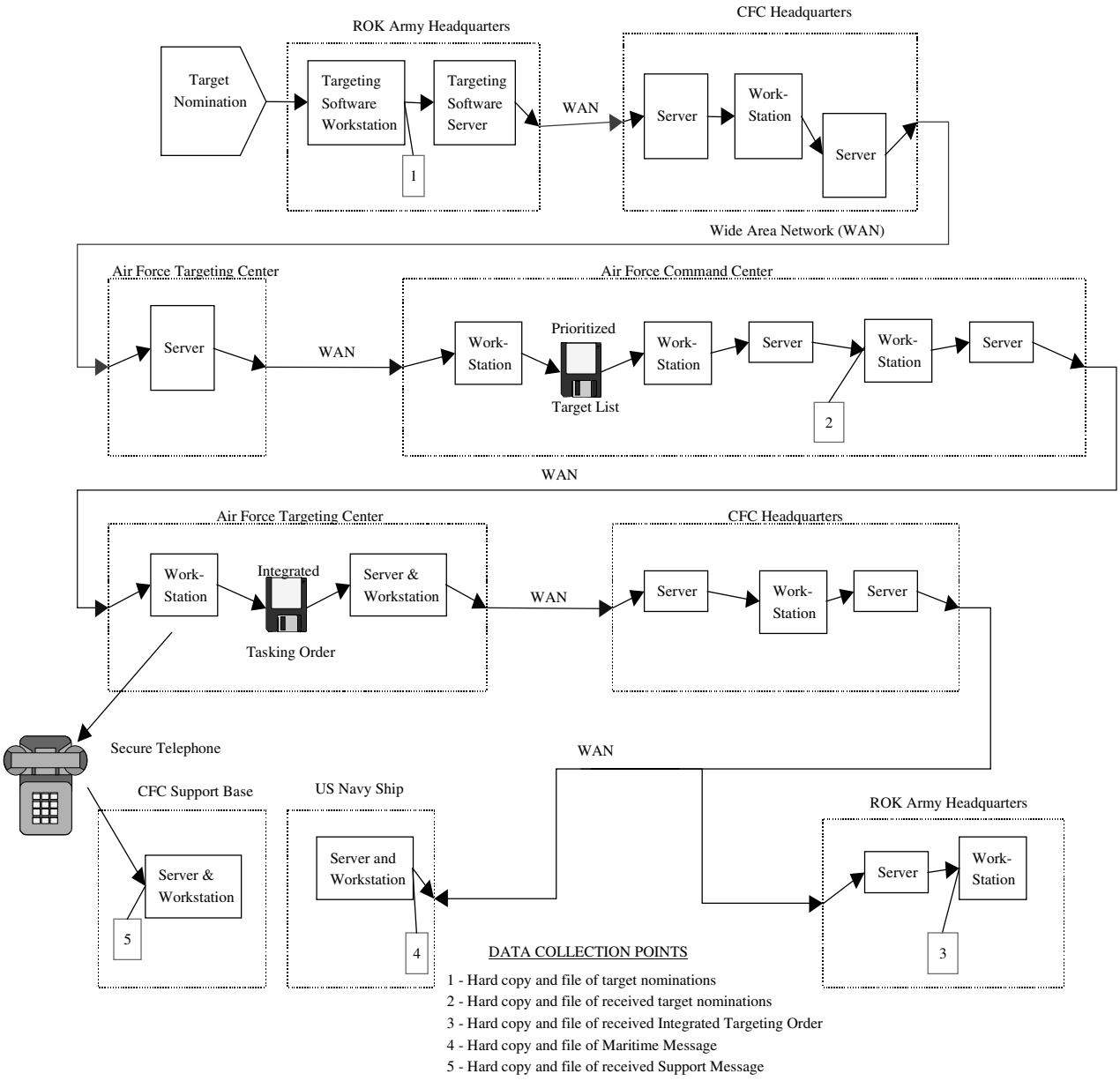

Figure 2. Data Flow/Bit Path for a USFK Targeting Mission Thin Line

Once the bit paths were developed, the USFK staff identified what products were needed and where to capture the products for evaluation. Bit paths were critical to the successful planning and execution of the evaluation because of multiple relationships within the thin lines of systems. Each mission could involve more than one thin line, each thin line could involve more than one task, and each task could involve more than one system.

At each data collection node along the thin line, the products were captured and examined against a variety of criteria for evaluating measures of performance; i.e., completeness, accuracy, and timeliness. Using these criteria, the data collectors and analysts could assess the thin lines for possible Y2K anomalies as they progressed through the clock rolls.

Throughout OPEVALs, evaluators at each command continued analysis of the products collected against performance criteria for completeness, accuracy, and timeliness to assess the presence of Y2K anomalies.

IV. OVERVIEW OF THE COMMANDS' OPEVAL ACTIVITY

The Joint Staff prepared an overall Y2K OPEVAL plan that gave the Unified Commands and Defense Agencies direction and form for establishing individual plans. The plan's goal was to make it possible to view interlocking systems and data flows for peacetime and wartime operations in a simulated Y2K environment. This was done to ensure that problems from the Y2K rollover did not adversely affect readiness and mission accomplishment. The combatant commands advised the Joint Staff on the progress of planning and evaluation results. The Joint Staff then compiled the information in a single data base, making it available to each of the commands and appropriate agencies. The Joint Staff also assessed proposed Y2K OPEVAL dates and intended content to recommend appropriate venues for integrating Unified Command events with several proposed Y2K Positive Response exercises.

OPEVALs started in December 1998 and continued through October 1999. By September, each CINC had completed at least two OPEVALs of its thin lines as directed by the Joint Staff. For some CINCs, a third OPEVAL provided the opportunity to test systems that were not Y2K compliant in prior tests, or that had been modified subsequent to earlier OPEVALs. Figure 3 shows the OPEVAL schedule for all CINCs. This table depicts the scheduled OPEVAL periods, but not necessarily the number of OPEVALs and activities that occurred. For example ACOM had two OPEVALs during the October period.

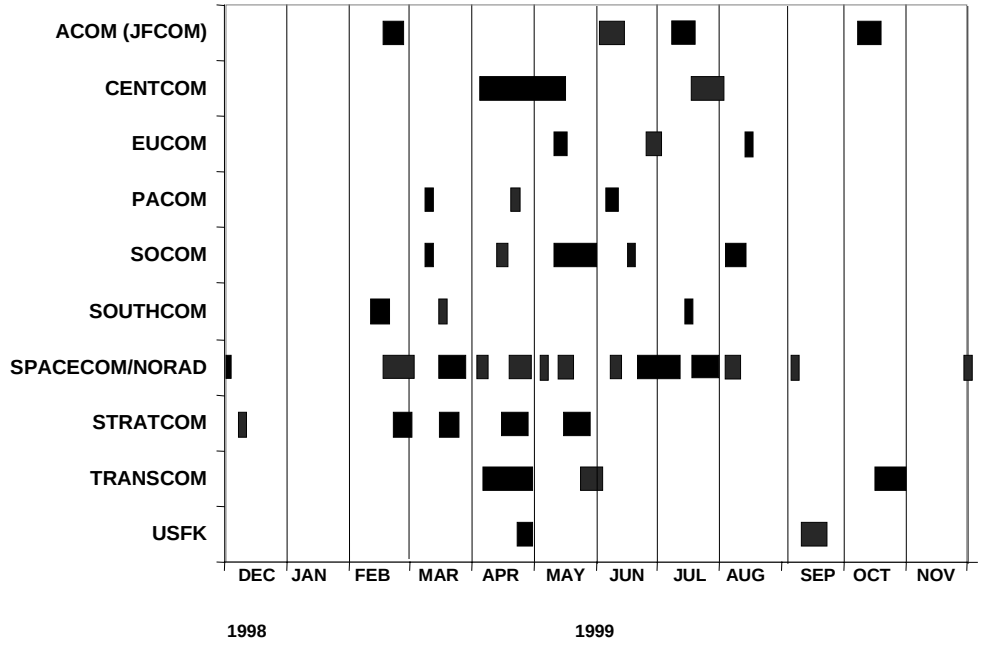

Figure 3. OPEVAL Dates

All CINCs retained a subset of their Y2K OPEVAL teams to practice the actions needed for actual rollover dates. These teams comprised the core expertise on duty at the rollover times so that they could correct problems that arose or implement operational contingency plans.

For each OPEVAL, the list of test events comprised the Master Scenario Events List (MSEL). MSELs covered the functional areas in each CINC's unified command as well as the subordinate component commands and a large geographic area.

Each CINC had roughly 200 events to execute, typically taking about eight hours. One command's OPEVAL, however, ran for several days. Figures 4 and 5 illustrate the extensive organizational and geographic breadth of CENTCOM OPEVAL 99-2 and USFK's September OPEVAL. Executed from July 15-31, 1999, CENTCOM OPEVAL included sites in the continental U.S. and Middle East, and spanned 13 time zones. The European Command, PACOM, and JFCOM also conducted OPEVALs that covered many time zones.

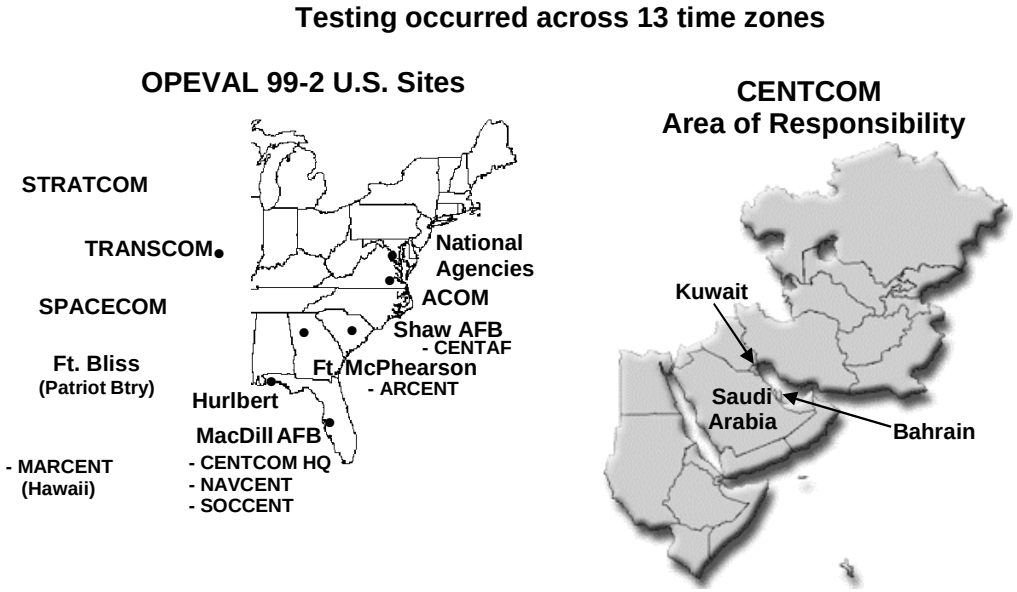

Figure 4. CENTCOM OPEVAL Over Two Continents and 13 Time Zones

During its September OPEVAL, USFK evaluated 33 major warfighting systems or applications at 11 separate geographical locations, including Republic of Korea Army and the 7th Fleet Command Ship at sea as depicted in Figure 5.

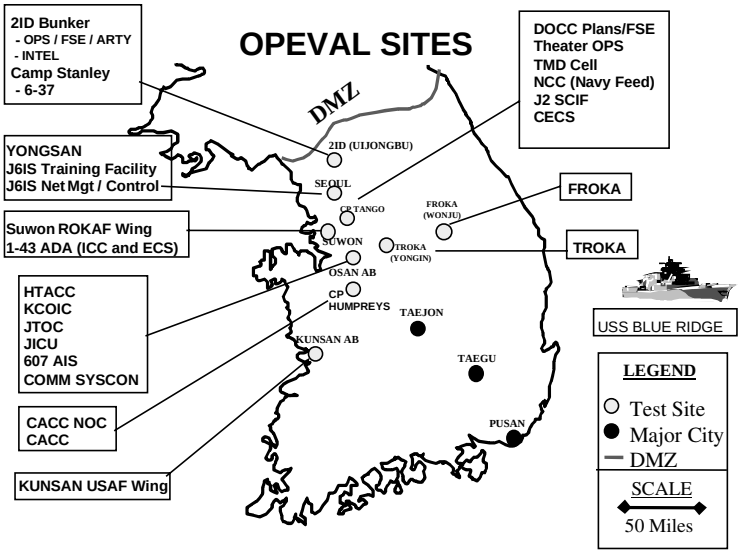

Figure 5. USFK OPEVAL Sites

In some cases, depending on the systems involved, the commands had integrated sensor and shooter computers into C^{4}ISR systems, and their interoperability could not be tested within the OPEVAL. Some commands tested directly with operational systems (e.g., SOUTHCOM). Figure 6 illustrates the elements participating in a SOUTHCOM OPEVAL focused on the drug interdiction mission. The evaluation included land-, sea-, and air-based sensors. The actual counter drug and intelligence systems were tested using redundant operational systems without creating a private, parallel network. The terminals were located in the command's Caribbean Regional Operations Center (CARIBROC) and the Joint Interagency Task Force-East (JIATF-E). Only minor problems appeared, giving the command high confidence that its equipment would work satisfactorily at Y2K rollover and beyond. These minor problems were corrected and no problems occurred during the actual Y2K roll over.

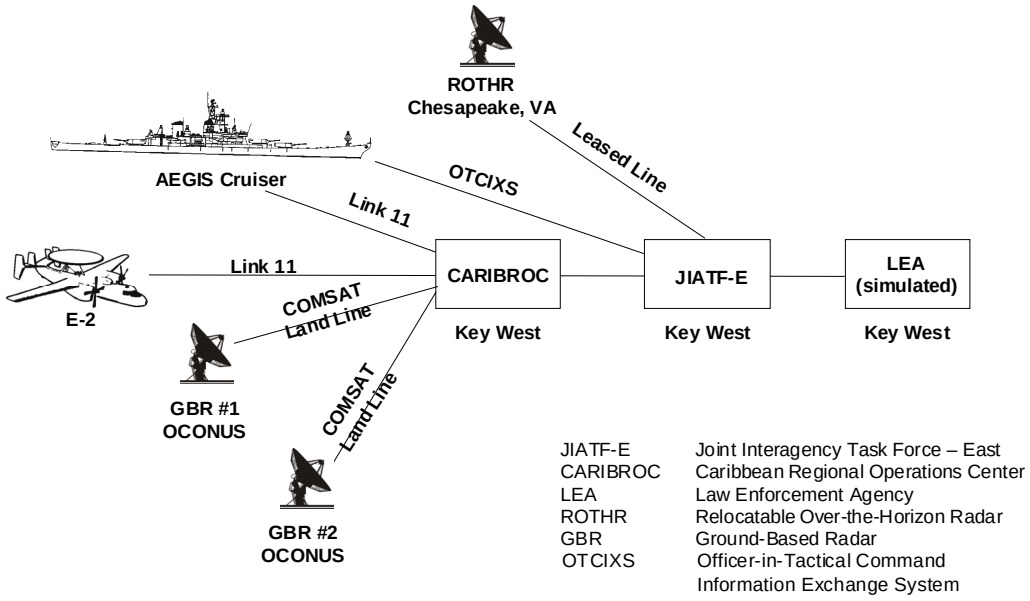

Figure 6. SOUTHCOM OPEVAL Scenario with Integrated Sensors

Typically, complex computer networks executed the operational scenarios for the OPEVALs. Figure 7 illustrates the network for TRANSCOM's OPEVAL-B, conducted May 24-June 4, 1999. In the figure, each box represents a geographically separate node with one or more local area networks. TRANSCOM integrated these into a system of systems using the operational backbone networks, the SIPRNET and the NIPRNET. For this and several other OPEVALs, NESs encrypted and decrypted data transmitted between test systems and sites. Operational systems did not access these NESs and thus could not read or be corrupted by test data.

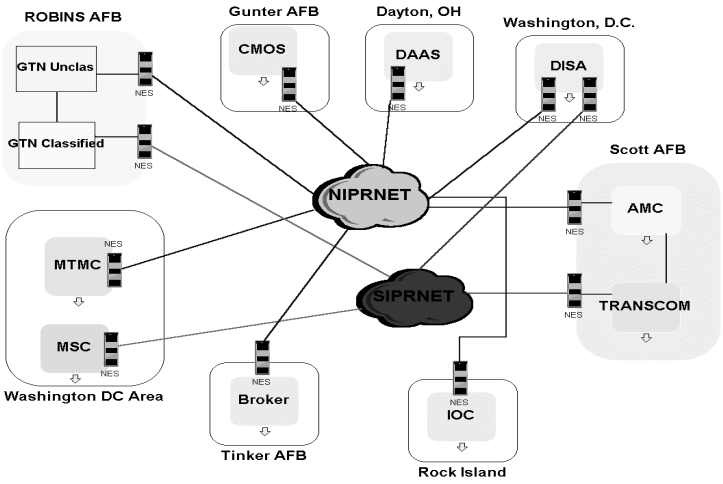

Figure 7. Networks Supporting TRANSCOM OPEVAL-B

In planning the OPEVALs, the CINC staffs faced several complex problems. Due to the need to retain the integrity of operational C^4ISR systems, the commands sought realistic alternatives. Usually, these alternatives used duplicate systems as a private network connected by the operational backbone communications network. To segregate the test data, and to prevent corruption of operational systems, many of the OPEVALs were conducted utilizing NESs when transmitting via the SIPRNET and other backbone communications networks. For example, in the TRANSCOM OPEVALs, the Global Transportation Network system at Robins AFB was the alternate to the operational system at Scott AFB. An exception to this rule was PACOM, where the operational systems used by an en route and in-place Joint Test Force headquarters were installed in an aircraft parked at Hickam AFB. Data were then transmitted between the airplane and PACOM headquarters. There were other exceptions as well, but they were based on risk mitigation to the CINC's operational mission at the time of the OPEVAL.

Each OPEVAL addressed a baseline date in 1999, plus three transition dates: December 31, 1999-January 1, 2000, February 28-29, 2000, and February 29-March 1, 2000. In most cases, the date rollover was "warm," where the test for the date included events before, during, and after the rollover. Since some system failures manifest themselves only during midnight transitions, most CINCs focused on the few hours prior to and the first hours after the midnight crossover periods.

The backbone communication systems and certain operational applications such as the Joint Worldwide Intelligence Communications System (JWICS), initially designated as trusted systems, were not assessed. Designating them in this manner left some uncertainty as to how well they would perform, but the major telecommunications companies had assured the public and DoD that their systems would be compliant. During later OPEVALs many CINCs used simulated SIPRNET, NIPRNET, JWICS, Defense Switched Network (DSN) and satellite communication (SATCOM) phone systems to the degree practical. Later, the Defense Information Systems Agency tested the DSN during summer 1999. Table 4

summarizes the communication backbones used for various OPEVALs. From Table 4, it is clear that, except for the foreign telephone networks, most systems were used by more than one CINC.

Table 4. Backbone Communication Systems Used in CINC OPEVALs

Command	SIPRNET/ NIPRNET	U.S. Telephone/Fax	Foreign Telephone/Fax	SATCOM	Other
CENTCOM	√	√	√	√	JWICS
TRANSCOM	√	√			
SOCOM	√	√		√	
STRATCOM	√	√		√	
JFCOM (ACOM)	√	√	√	√	JWICS
SOUTHCOM	√	√		√	LINK 11, OTCIXS
USFK	√		√	√	RELROK WAN
PACOM	√	√	√	√	AUTODIN, DSN, JTF-
EUCOM	√		√	√	DSN, JWICS

V. SUMMARY OF RESULTS

Overall, Y2K OPEVALs were very successful—they uncovered problems—virtually all of which were corrected to eliminate actual Y2K flaws. OPEVALs detected several software problems that were easily corrected and verified in subsequent OPEVALs. The biggest value of the OPEVALs was the knowledge learned getting ready for them; i.e., defining baseline capabilities, identifying thin line critical systems and interoperability implications, isolating and identifying interoperability problems, and developing contingency procedures. The CINCs weeded out some of the old and obsolete systems, and now have a much better understanding of interoperability in their C^4ISR architectures.

The CINCs found that they could perform their critical missions during and after Y2K date changes. The tests found several problems with thin line systems, both Y2K and non-Y2K related. These problems were generally resolved using alternate systems, plus manual procedures short of full contingency plans. Y2K problems consisted of three types. Some were system interoperability failures, in which each of the two systems operated as intended but still had Y2K interoperability problems. In other cases, systems and peripherals such as printers did not interoperate properly. Systems previously certified as Y2K compliant had newly identified Y2K system failures. These problems consisted of simple things such as incorrect dates on message headers or facsimile transmissions, with no other effects on content, function, or operation. In some cases, the problems were severe enough to cause incorrect transmission or exchange of data or imagery.

Non-Y2K problems discovered during OPEVALs centered on issues of configuration management and the tendency for personnel to install new versions of a variety of applications or systems on their computers without regard to joint interoperability problems. Non-Y2K issues also included previously unrecognized, everyday midnight crossing anomalies, obsolete software on particular installations, and known bugs to be corrected in software updates. Usually, the non-Y2K problems were corrected prior to the end of an OPEVAL, but configuration management difficulties were a major area requiring the commander's attention. The list on pages 2-3 summarizes the systems and applications most commonly encountered throughout the several commands.

Each of the 358 mission critical systems was tested at least twice, either in CINC OPEVALs, Service tests, or Agency tests. The CINCs had the authority to use each other's test results if that test accurately represented and supported their thin lines and critical supporting missions. Table 5 depicts the

system test breakout by CINC for the first and second tests. The number in the CINC column denotes the number of systems that each CINC tested in his OPEVAL program. Numbers in other columns are tests conducted by other CINCs as a by-product of their evaluations, tests by the Services, or tests by the DoD Agencies.

Although the OPEVALs were very successful, they did not assess all possible interactions. This was due to the need to prevent degradation of current warfighting capabilities. However, USFK, CENTCOM, and SOCOM came very close to using all of their operational systems in their OPEVALs, which helped further mitigate risks.

Several long-term benefits derived from these evaluations, arising primarily from the information management system methodology developed during the OPEVAL process. As a result of this synergistic effort, a baseline now exists which reflects current C^4ISR operational and system architecture and software configuration. Using the current baseline architecture as a starting point, the CINCs can make reasonable decisions concerning their disposition of obsolete systems and plan their acquisition strategy for the future. Additionally, the CINCs gained valuable knowledge about internal warfighter operations and external interoperability issues. Valuable information was gained which supports the need for strong and continuing configuration management of operational systems within their organizations, including the organizations they communicate with. In addition, joint interoperability problems were discovered, highlighting the need for attention to system and software compatibility, as well as the mission critical tasks enabling successful execution of joint operations. Where necessary, the commands created workarounds or operational contingency plans, which were evaluated and in place for Y2K rollover times.

Table 5. CINC First and Second Test Coverage

CINC	SYSTEM FIRST TEST						SYSTEM SECOND TEST					
	CINC	OC	SER	AG	UNK	Total	CINC	OC	SER	AG	UNK	Total
STRATCOM	101	14	9	5	0	129	47	19	53	10	0	129
SOCOM	58	13	0	1	0	72	29	19	19	5	0	72
JFCOM	40	17	3	6	0	66	4	35	12	15	0	66
CENTCOM	54	6	1	4	0	65	13	35	8	9	0	65
EUCOM	30	17	1	0	0	48	4	26	11	5	2*	48
PACOM	16	14	9	2	0	41	9	16	13	3	0	41
SOUTHCOM	20	5	0	0	0	25	4	15	0	6	0	25
SPACECOM	47	9	5	7	0	68	40	15	8	5	0	68
NORAD	29	20	5	0	0	54	15	13	25	1	0	54
TRANSCOM	27	8	0	2	0	37	23	12	0	1	1**	37
USFK	26	0	1	0	0	27	9	8	9	1	0	27
Total	448	123	34	27	0	632	197	213	158	61	3	632

Legend: * = One blank for a second test; One annotated that no test required
** = One blank for a second test
CINC = System tests conducted by the designated CINC
OC = Other CINC conducted the test
SER = Service element conducted the test
UNK = No entry
AG = Agency conducted the test; e.g., DISA, JUSE, NIMA, etc.

The Joint Staff and CINCs should consider using this evaluation methodology within their exercise frameworks. As a minimum, periodic OPEVALs that produce an understanding of system capabilities should be institutionalized. It is ironic that the greatest benefit from the operational

evaluations—verifying interoperability and correcting interoperability problems—would have received little support had they not been driven by the Y2K issue. As a result of the OPEVALs, we now have much greater confidence that the thin lines of C^4I systems will perform as intended in war or contingency. DOT&E will continue to support future CINC efforts to ensure C^4I interoperability.